REMARKS/ARGUMENTS

Allowable Subject Matter

The Examiner is thanked for the indication of allowance subject mater in terms of claims 5-10, 19-24, 29, 32-34. However, as will be seen in the discussion below, the applicant believes that all of the claims presently define over the cited art.

Claim Objection

The Examiner objected to the use of the phrase "of the or each" asserting that the phrase in claims 5, 8 and 29 is allegedly "grammatically incorrect". With all due respect, the applicant disagrees with the assertion that the term is grammatically incorrect. It is noted, for example, that this phrase (or just "the or each") is rather commonly found in issued US patents. See, for example, 6,401,671; 6,579,258; 7,273,429; 7,212,634; and 7,225,919. Given the acceptance of this form of expression in issued US patents and given the fact that the Examiner has cited no document in support of his assertion regarding its alleged lack of grammatical correctness, is it respectfully suggested that the assertion should be properly withdrawn.

Claim Rejections - The Pienado Reference (US 2002/0013722)

Basically, according to this document, a user can download encrypted content to a user computing device from a content server, the content being encrypted under a symmetric key KD. This key is associated with the content and with applicable license terms in a content-key database 20. The user computing device includes a trusted DRM subsystem that includes a "black box" (obtained from a black-box server 26 – see Figure 1); this black box has its own public/private asymmetric key pair (PU-BB-CO / PR-BB-CO where PU

apparently stands for 'public', PR for 'private', BB for 'black box' and CO for the user's computing device).

To access the content, the user must obtain a license from the license server which, after checking the user's computing device is trustworthy, gives the user's computing device a license including the key KD encrypted under the public key PU-BB-CO of the black box of the user's computing device.

The black box in the user's computing device can now recover the KD by using its private key PR-BB-CO. However, before using the key KD to decrypt the encrypted content, the black box awaits confirmation from a license validator of the DRM subsystem that the user's computing device satisfies the license terms (see paragraph 0200 of Pienado).

The Examiner cites the embodiment of Figure 13 of Pienado in which the encrypted content and a sub-licence are passed to a portable device from the user's computing device. The portable device has a cut-down version of the DRM but this has its own black box with a respective public/private key pair PU-BB-PD / PU-BB-PD. The sub-license includes the key KD that has been re-encrypted by the user's computing device (after decryption) under the public key PU-BB-PD thereby enabling decryption by the black box of the portable device.

Differences between Pienado and Claim 1

The Examiner may have misunderstood Pienado since the first three lines on page 3 of the Official Action the Examiner appears to be saying that Pienado discloses content encrypted according to encryption parameters comprising:

- PU-BB-PD (supposedly the "public data of a trusted party" of claim 1), and

• KD (supposedly the "encryption key string" of claim 1).

However, no indication could be found in Pienado that the DRM protected content is encrypted other than under the key KD – the subsequent encryption of the key KD itself under PU-BB-PD is clearly not relevant here since that is encryption of a key (KD) rather than the DRM protected content. Paragraphs 0300 to 0302 of Pienado describe how the portable device renders the content and clearly the DRM protected content is only encrypted under the key KD as described in paragraph 0302 of Pienado.

The Examiner's argument thus fails at virtually the first hurdle of claim 1 as Pienado does not disclose encrypting data "based on encryption parameters that comprise: public data of a trusted party, and an encryption key string ..." as required by claim 1.

Another difference between claim 1 and Pienado is that claim 1 calls for the second computing entity to "generate" the decryption key (note the recitation that "the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data" in claim 1) whereas Pienado clearly only recovers KD by decryption (in particular, the user's computing device recovers KD using PR-BB-CO and the portable device recovers KD using PR-BB-PD).

Actually there is a more fundamental problem with the Examiner's argument: since the Examiner tries to equate the decryption key KD of Pienado to the encryption key string of claim 1 (as he does) then it is pointless to try to find in Pienado disclosure corresponding to the following claim 1 passage:

"the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data"

because, if the second computing entity has the encryption key string, it already has the decryption key since in Pienado the key KD is a symmetric key - see paragraph 0285 of Pienado.

Withdrawal of the rejections and allowance of the claims are respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2125. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2125.

I hereby certify that this correspondence is being transmitted by facsimile transmission to Commissioner for Patents at 1-571-273-8300 on

October 10, 2007
(Date of Transmission)

Valerie Hay
(Name of Person Transmitting)

Valerie Hay
(Signature)

October 10, 2007
(Date)

Respectfully submitted,

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile